Full Risk Assessment

Identify and Assess Risks

Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your proposal are considered. If you run out of space then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

Examples of **risks to individuals** include**:**

- Discrimination
- Identity theft
- Financial loss
- Reputational damage or embarrassment
- Physical harm
- Wrongful arrest or prosecution
- Loss of confidentiality
- Inability to exercise rights

Examples of **corporate risks** include:

- Failure to protect the public
- Loss of public confidence
- Civil litigation
- Reputational damage
- Regulatory action
- Breaching other legal obligations

You should identify **solutions** such as:

- Deciding not to collect certain types of data
- Reducing the scope of processing
- Reducing retention periods
- Taking additional technical security measures
- Following approved codes of conduct
- Restricting access to data
- Training staff to understand the risks
- Anonymising or pseudonymising the data
- Using different technology
- Using an alternative third party processor

9.1 Data Protection Principles

1. Fair and Lawful

- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected and recorded?

2. Purpose Limitation

- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation

- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy

- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Retention

- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all systems if required?
- Is the retention period necessary and proportionate?

6. Security

- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights

- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to the DPO.

Describe the source of risk and the nature of	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
	1 - Rare *2 - Unlikely*	*1 -* *Insignificant*	*Very High* *High*	*Describe the mitigation and whether it will be implemented*	*Is the risk:* *- Eliminated*	*Very High* *High*

potential impact on individuals.	*3 - Possible* *4 - Likely* *5 - Almost Certain*	*2 - Minor* *3 - Moderate* *4 - Major* *5 - Critical*	*Medium* *Low* *Very Low*		*- Reduced* *- Accepted*	*Medium* *Low* *Very Low*
Purpose limitation: results used for a different purpose than project purpose	1	3	Low	We will ensure that the work's results are quality assured and peer reviewed. Any significant outputs will be documented in a single source of the truth, which will also include any assumptions, caveats and limitations in relation to the outputs. Be very clear about who the cohort are to ensure there is no expectation for this work to be applied at police level. Set a high expectation for transparency with the steering board. Save all code in Github to enable reproducibility and audit.	Reduced	Very low
Purpose limitation: function creep	1	2	Very low	The project has very specific aims and its funding is signed off for limited time only. We plan to delete all police data (both raw and any derivatives) once the project is finished. Any further analysis using this data will go through another DPIA process.	Reduced	Very low
Data minimisation: data is processed unnecessarily	3	3	Medium	Data analysts met with an SME at GMP who understands their data well. Together they created a list of variables for exploration purposes, where there was an expectation that all selected fields have some predictive power. During the analysis stage of the project any variables that are redundant will be removed from the models. Feature selection will be performed by considering the pairwise correlations, VIF, p-values and mutual information, as well as contributions in best-preforming models.	Reduced	Low
Accuracy: quality of data is not perfect	4	2	Medium	During the data discovery phase any variables that are of very poor quality will be discarded. Analysts will make appropriate judgement on the type of post-processing (e.g. imputation, record deduplication and removing of inconsistencies) that is suitable for each data field. Any assumptions and actions will be recorded in the final report.	Reduced	Low

Retention: data is not disposed within agreed timelines	2	3	Medium	The MOJ has semi-automated processes to track retention periods. Any extension to these periods will be sought via additional DPIAs.	Reduced	Very low
Security: data breaches	1	4	Low	The Analytical Platform at MOJ has high security safeguards in place. In addition, the team uses packages and gitignore files to strip any data from code scripts.	Reduced	Very low
Security: loss or interception of data	1	5	Low	The project uses a Government tool, the data uploader, which has security guarantees and strict governance measures, which include: encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems.	Eliminated/Reduced	Very low
9.2 Data Sharing - including the involvement of other Controllers and Processors						
- What contracts, MOUs etc are in place or may be required? - What measures have you taken place to ensure third parties comply with Data Protection laws?				- What risks are involved with sharing data? - Is sharing necessary and proportionate? - Is the sharing of data being minimised?		
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**
Police data differing between GMP, PNC and MOJ versions	3	2	Medium	This is a risk to the project success and therefore project ambition will need to be scaled down if the data available is not appropriate. In the eventuality that there is no sufficient data to develop any model then the project will end early. The DPIAs and DSA with GMP will contain similar information and aims whilst still adhering to their specific conditions.	Eliminated	NA
9.3 International Transfers						
- Will data be shared with a third party based outside the EU? - If you will be making transfers, how will you ensure that appropriate safeguards are put in place?						
Describe the source of risk and the nature of	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation/ Solution**	**Result**	**Residual Risk**

potential impact on individuals.						
Data will only be transferred between GMP and Ministry of Justice – all based within the UK. However, data will be stored on a server using AWS based in Ireland, EU.	1	4	Low	Safeguards are built to deal with the management and transfer of official sensitive data. The platform follows NCSC Cloud Security Principles, implementing features such as: • 2 factor authentication for user sign-in • encryption of data at rest and in transit • fine-grained access control • extensive tracking of user behaviour, user privilege requests/changes and data flows • multiple levels of isolation between users and system components • Web access firewalls • Cloud trail and lambda upload cloudwatch log • Storing data in S3 buckets and managing access using project access logs needing two independent approval levels	Reduced	Very low

9.4 Additional Risk Factors

Describe any further risks, ensuring that any risks not already identified are included.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
Organisational risk: public not agreeing with the aim of the project	1	4	Low	The project was commissioned directly by the Prime Minister's office and approved by the Crime and Justice Taskforce. The analytical team engaged with both Manchester Police and Manchester Probation colleagues via a workshop to scope out the specific project aims. A working group is also invited to comment on the project's progress regularly.	Reduced	Very low

Operational Data Risks - Additional Risks Relevant to Operational Data Only

This section is only applicable to proposals involving operational data. **If you are solely processing administrative data then do not complete.**

10.1 Data Logging

Where data is processed electronically then logs must be kept for certain actions. This is to enable effective audit of processing systems, data sharing, and to verify ongoing lawfulness of processing.

If the data is processed electronically then will a log be retained of the following actions:

• **Collection** • **Alteration** • **Consultation** • **Disclosure** • **Combination** • **Erasure**	☐ Yes ☐ No* ☐ Not applicable *****If you answered “no” then you must record this as a risk below.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk
N/A	-	-	-	-	-	-

10.2 Data Categorisation

When processing data for law enforcement purposes, you must **provide where relevant and as far as possible** a clear distinction between categories of data subject.

Will there be a clear distinction between different categories of personal data suspects, for example subjects who are:

• Suspected of having committed, or are about to commit, a criminal offence • Convicted of a criminal offence, • Victims of a criminal offence, • Witnesses to a criminal offence.	☐ Yes ☐ No* ☐ Not applicable If you answered “no” then you must record this as a risk below.

Describe the source of risk and the nature of potential impact on individuals.	Likelihood of harm	Severity of harm	Initial Risk	Mitigation/ Solution	Result	Residual Risk